Hiring to Firing Podcast – Episode 3

Title: "What Can *Squid Game* Teach Us About Confidentiality Agreements and Restrictive Covenants?"

Speakers: Tracey Diamond, Partner at Troutman Pepper and Evan Gibbs, Partner at Troutman Pepper

Special Guest: Richard Eskew, Executive Vice President, General Counsel and Chief Compliance Officer at Accolade

Date: July 19, 2022

[TRACEY]

Welcome to *Hiring to Firing* the Podcast. Today, my partner, Evan Gibbs, and I welcome Richard Eskew, who is the Executive Vice President, General Counsel, and Chief Compliance Officer at Accolade. Accolade is a company that provides personalized healthcare services to help each member find the right care at the right time to improve outcomes, lower costs and make better healthcare decisions. In his role, Rich is responsible for the company's legal compliance and security functions. Welcome, Rich.

[RICH]

Hi Tracey. Thanks for having me. Evan, thank you as well.

[TRACEY]

So, let's get started by talking about the hit TV show, *Squid Game*. *Squid Game* is a story of a group of down-on-their-luck players who accept a strange invitation to compete in children's games. The games are staffed by masked workers in red jumpsuits, identified by a circle or square shape on their covered forehead.

[Video Played]

[Speaker 1]

I would like to extend a heartfelt welcome to you all. Everyone here will participate in six different games. Over six days. Those who win all six games will receive a handsome cash prize.

[Speaker 2]

And why should we believe that? You took all our stuff and put us to sleep coming here? And then you brought us to this strange warehouse. Now you're saying, you'll pay us if we go and play a few games. You really expect us to buy that?

[Speaker 1]

We reluctantly took all of those measures to maintain confidentiality as we brought you here.

[TRACEY]

For those who have watched the show, you will agree that *Squid Game* certainly takes a concept of confidentiality to its extreme. Going so far as to shoot a worker who removes his mask. In real life, why is confidentiality in the workplace so important?

[RICH]

Thanks, Tracey. Confidentiality in the workplace is critical because when you think about everything that we do as a business and to fit in our planning stages, and, you know, how we strategize where our business is going to go. Accolade is lucky enough to be in a really big and growing industry, but also one that's seeing a lot of convergence. And so, the confidential information about how we're innovating our service, you know, sort of the secret sauce of how we think we get to better outcomes for individuals from a health perspective. And we're just generally strategically, we're going, that's all our confidential information. It's something, you know, we work really hard to develop and therefore want to protect. So confidential information is critical for many businesses.

[TRACEY]

Accolade is an interesting company to talk about confidentiality because you have so many layers of it. You have the personal health information of your members that you're dealing with, as well as your own technical and financial, and strategic information. What type of information are most companies concerned about keeping confidential, generally speaking?

[RICH]

There's the traditional, you know, forms, you know, financial business information, strategy innovation. Obviously, if you have trade secrets in your business, the things that give you a competitive advantage against your competitors and that you really closely guard, those are the traditional forms. You're right to mention that for Accolade, there are many, many layers of that. You know, our business is built on trust. If you understand a little bit of what our business is about, we're here to support members in navigating the really complicated healthcare system. And part of the way we do that is by building a long-term trusted relationship. And so, you know, the data that we have on a particular member, which is typically very sensitive because it relates to their healthcare, it's really important that we maintain confidentiality and privacy and have really high standards for security for that. Because if you, if we don't protect that information, you know, we can't build that long-term trusted relationship with an individual.

So, we have all the traditional confidential information that you might expect companies to have. And then we have that additional layer and it gets complicated when you think about how that information does need to flow in certain ways through the healthcare system, in order for people to actually access care while also maintaining a high level of privacy and security on that information and the interplay between that individual who may be an employee or dependent of an employee and their employer/employee relationship with the company that has engaged Accolade to provide that service. And one of the benefits we can provide is the ability to be an independent resource for that individual. And so, keeping that information confidential from their employer is really critical for us.

[TRACEY]

So. you're talking about keeping confidential information of your members, the ones that you're working with to help them maximize their benefits from their own employers, which are your customers. You're not talking about your own employees, right?

[RICH]

Yes. As to our customer employers, but also our own employees as well, especially as we look to provide a, you know, the accolade service to our employees, it creates special concerns and challenges in that regard. But again, all in the vein of having those zones of confidentiality and those trusted relationships with anybody who we would call our members.

[TRACEY]

I want to get back to employee information in a second, but let's pull Evan into the conversation a little bit. Evan, can you, you do a lot of work in this area. Can you explain to us what the difference is between confidential information and trade secrets?

[EVAN]

Yeah, yeah, sure thing. I mean, so, you know, confidential information is generally something that party who owns some information can define itself. You know, they first of all, they have to identify what they consider confidential to their business. And then second, they have to generally take some kind of measures to make sure it's actually confidential. You know whether it's, you know, user restrictions or labeling stuff, you know, confidential or whatever. And then that stuff, stuff that is considered confidential information is what we usually see protected by contractual terms. You know, so non-disclosure agreements, confidentiality provisions, and employment agreements or severance agreements, you know, things like that. And it can be really, and I typically see it, you know, very broadly defined. Then you've got trade secrets and those are, you know, statutory definitions. You've got the uniform trade secrets act and then you've got the defend the federal defend trade secrets act. And they all pretty much define trade secrets the same way. And it's a higher threshold than confidential information. But a lot of times it's, it's not necessarily that hard. And I think that what surprises, most people when I talk to folks, especially employees or employers who have received alleged trade secret information from a competitor, is people are often surprised at how low the bar can be for something to be a trade secret. If a company, for example, has some kind of, you know, template document that it uses that it's developed over a number of years or some kind of procedure manual, you know, stuff like that, stuff like that can absolutely qualify as a trade secret. So, there's a real distinction, but I don't think the bar is as high as a lot of people think for something to be a trade secret.

[TRACEY]

Yeah. That's really interesting what you just said about template documents. I had a case very similar to that where an employee took template documents with him because he wanted the templates to use in his new company because he doesn't want to have to sort of re-create the wheel. He wasn't looking to take the prior employer's confidential information per se. He thought of this as his own work product and the company, our client really was upset about it because they felt they're taking, he was taking their work product and, and pretty much giving himself a leg up with their competitor company. You know, Rich, what do you think about that? And what do you do to sort of safeguard against that? Or do you allow employees to take it?

[RICH]

I think the key for me. and these are best practices. I think Evan's exactly right that the bar can be low. But I think as a company, you think about, you know, your best practices and if you think you've got trade secrets, you know, for me, one of the best practices is to make sure your employee is aware of what those things are. Obviously, you have to take all the other precautions. Limit access, right? Not every employee should have access to something that you might consider a trade secret that would sort of defeat the sort of least privileged access motto. But you want to make sure those employees who do have access to that know that this is even beyond may be confidential information. This is something the company believes is its trade secret information. And so, we try to really help our employees through training, our policies and procedures, understand what is confidential. And then what are those things that may even rise to the level of a trade secret?

And I think then you, you get on level footing with employees and what we find then you also, you also have a culture of open communication. Then if an employee's going to leave and wants to take something like a template where there might be a question about whether or not the company cares so much, we can have an open conversation and either advise the employee, no, they can't take that

with them. Or, you know what, yeah, we'll let you take that with you, because we don't believe that that is truly confidential or trade secret to the business. And I think those are some of the best approaches when you're trying to do this effectively with a wide array and a large number of employees.

[TRACEY]

You know, *Squid Game* is a good example of that because there's so many layers of confidentiality within that company, right? There is the contestants that are kept completely in the dark. They're the worker bees that are kept somewhat in the dark. And we still don't yet know, I'm wondering whether they're going to develop this more in a future season. We still don't yet know where those worker bees are coming from, whether they are, you know, prior winners or, you know, where are they pulling these people from? Cause they're certainly not treating them very well. And then there's another, a layer of supervision. I forget whether it was the circle or the square on the face, that was the supervisor and then all the way up sort of through to the top layer. And then the the top guy really is not giving very much information to any of his underlings. So, confidentiality sort of up the pole and then down the pole, again. Can a company go too far and in keeping things so confidential that they're making it too hard for people to do their jobs?

[RICH]

No question about it. And, and as you were speaking, Tracey, I was thinking about my next comment being, you know, companies today, having high employee engagement and making and helping your employees feel, you know, part of the business and engage with the work that they're doing, really being able to see how their work, uh, produces outcomes for the business. That's what creates joy in somebody's job. And so, there's a tension there with, you know, overly policing the way you, you handle confidential information and even trade secrets. And so, on the, on the one side, we're talking about the extra measures and steps and, and things you take to protect confidential information, but for sure, you can pull that too far and you can start to chill your employee's ability, not just to do their jobs, but also to become engaged with their work. And so, it's a really key balance that I think, you know, companies and certainly, you know, something that we try to practice at Accolade, really to stay focused on that tension and finding the right balance at all times. And, and I think companies can't be afraid to constantly assess themselves against that standard to make sure they're striking as positive a balance as they can. But you can certainly take it too far.

[EVAN]

I would say, you know, for me, one thing I would love to see companies do that I've really, I've never heard, I've never had a client, or I've never read about a company having a policy or practice of specifically advising employees that things that they create when they're at work on behalf of their employer, it's not their personal property. You know, because that is, I mean, in 100% of the cases I've litigated, that is the story that people always say. They say I made this as part of my job. It's mine. It's not theirs. You know, I developed this template over a, you know, a decade of working for this company. It's perfect. And, it's mine, you know, or, you know, the one that is ubiquitous is this is my client list. These are my clients. They're not my former employer's clients. And in terms of restricting access and stuff like that, I do see that, that tension. I mean, it's, that's very real. I would, I honestly feel that if companies took that other step of telling folks, regardless of, you know, what level of restrictions they have on access and stuff if they really made it abundantly clear to employees, that stuff they create is not theirs, I think that could go such a long way. Because I mean, I really, I mean every time somebody says that I can tell they genuinely believe it. They're not trying to sort of come up with a sort of post hoc justification for, you know, wrongful conduct. They knew was wrong. It's always, they genuinely believe that it's theirs and they can have it.

[RICH]

It's a great point. You know, I'll tell you, you, your, Troutman Pepper has one client that, that does try to do this. <laugh> that, and that's, that's Accolade. You know, we, in addition to what I'll call our formal policy or the formal sort of confidentiality invention assignment type agreement that many, many companies have, we try to have a guide also to that. And then, and then we try to explain to employees and, and, and again, create that open communication about these kinds of things, both when new employees come in, we see often certainly as a company, we don't want any employee bringing the confidential information of their former employer. And I saw this a lot. I used to be in the investment banking and financial trading markets. And so, we would see a lot of times traders would bring algorithmic spreadsheets with them.

And the first question, number one, our policies and procedures would say, well, you need to disclose anything that you're going to bring in that comes from the outside because we need to evaluate exactly this question. And then we would get into a conversation sometimes involving the former employer that said, “Hey look, um, Jane Doe has this algorithm. Jane is saying that they, this is you've agreed that they own this”. And we confirm that. And then we would, you know, either find out that no, that the former employer disagreed, but actually most times the employee was trying to do the right thing and did, in fact, have the former employer's approval to bring that in. And then we would work out with them. Well, what you're bringing to us on day one, we recognize as yours, you haven't created that while you're on our dime, so to speak.

And so, what we would do is we would actually, this is in the old days, we would put it on a CD ROM and we would escrow it. And say, look, when you leave that company, you can take that thing with you. But everything you develop on top of that, we're going to be able to retain. It's going to be ours and we're going to be able to retain that. You can't stop us from using this algorithm because we're hiring you to build a team out that does these things. There's a bunch of manifestations of how that kind of conversation can play out, but I think Evan, to your point, it's really important to get a company to that place where it can be identifying those things and then really practicing them. Having an agreement that says one thing, you know, many agreements have the attachment that says disclose all your prior developments, no one almost ever fills it out unless the employee is sensitive to it, and it goes into a file drawer and collects dust. We try to make sure we elevate those things into our actual practices. I think it's super important and your point of

[EVAN]

I'm very impressed. I'm very impressed. I love to hear it.

[TRACEY]

I was just thinking it's a much more sophisticated approach than a blanket. Don't bring anything with you from your prior employer. Going back to a point that you had before Rich about confidentiality going too far, where employees don't have access to the bigger picture of what's going on. And you were talking about how that creates sort of an unmotivated workforce. I think it also could be negative for the supervisors or for management because they're not getting access to the employee's ideas on how to make the bigger picture, more successful. So, sort of cutting off that access goes both ways. I also wanted to get back. This is going back a bit, but Evan, you had mentioned something about the Defend Trade Secrets Act. And I think sometimes companies are a little confused about that one. It's a little more recent. Can you explain to you what the difference is between that federal statute and, and sort of state trade secret laws and why an employer may want to make sure that they're eligible to take action under the federal law?

[EVAN]

The main sort of thing that the Defend Trade Secrets Act did was give a federal cause of action to get the parties into federal court. So, it depends on which side of the case, you're on that, it's either a really good thing or a really bad thing. The definition of a trade secret and all the other, you know,

sort of provisions the attorney's fees provision, which I will point out something that I realize that recently a lot of people take for granted, but the Defend Trade Secrets Act, there's an attorney's fees provision to it. Right? But what a lot of people forget is that to get, to be entitled to attorney's fees and exemplary damages, you have to show that the conduct was willful and malicious. And I just want to point that out because I've had some litigation recently where parties assume parties on the other side of a case assume that they were going to get attorney's fees. For example, the Fair Labor Standards Act, you know, it's a, it's a much lower bar. You essentially just have to be successful in the case and you get attorney's fees, but it's a much higher threshold to be entitled to attorney's fees. And it has to be willful and malicious. It's not willful or malicious. And so that's a pretty high standard. So that's, I just a, just sort of a practice point. I just want to throw it out there.

[TRACEY]

Willful and malicious, you really have to show that this is a bad actor.

[EVAN]

Yeah, that's right. That's right. And there was a, there was a case recently, you know, Tracy, you actually shared it with me that you don't see very often, but I think is also a really good point is people also forget there's a, there's a criminal component to the Defend Trade Secrets Act. And Tracy sent a case. There's a, I mean, there's a recent case from earlier this month where that sort of scenario we're talking about. These two individuals were employees at a biotech company. And essentially as employees took a bunch of information, retained it, put it on personal devices, etc. And then they moved to another country and founded another company on their own using the exact trade secret, you know, all of the data from this former company to generate a competitor. And they actually went out and got like a 100 million investment in this new company and then low and behold, you, they sort of get up and up and running and their former employers like whoa now. And so those two folks were convicted criminally under the Defend Trade Secret Act. Again, there's some other, other statutes as well, but you know, it just goes to show that folks do need to tread lightly when they're thinking, but there can be, there can be serious, you know, more than just sort of the new employer gets, you know, has to pay some money. I mean, it can be, you know, some very real personal penalties for the individuals involved as well.

[TRACEY]

People that are in HR, your HR, you know, folks are wearing many hats and there's always a tension between, you know, being there as a coach and assisting employees, disciplining employees, making or assisting with termination decisions, helping to administer benefits to employees. And HR as a department gets a whole lot of information about employees, personal information about their birth dates or social security numbers, health related information, etc. How does an HR department navigate that? Where you have to be careful that they're not using the information that they have in their files to misuse, you know, misuse that information at the expense of the employee?

[RICH]

For me, everything starts with having the right policy, but then bringing that policy to life through training and communication. And then there are some structural things you can do. The Benefits Team is maybe reports up organizationally to the same head of HR but is separate from the Talent Acquisition Team and some of the other teams that might have different functions and you make sure that you have role-based access so that, you know, some of that more sensitive information in the benefits space isn't crossing over into the people in HR that, you know, the business partners that support maybe performance management or the talent acquisition folks who, who help the business, make decisions about who they're going to hire on the inbound front. And so, there's, you know, there are some systemic things that you can do, but then there's also that, that training and, and having the correct policies.

But I think the philosophy is we talk about trust a lot in our business, not just with our members and our customers, but with our employees, right. They are the engine that enables us to do great by our members and our customers. And so, you know, we want them engaged in their work. We want them to be trusting of us as an employer and that requires communication, but it also requires that they trust that we have their data secured in the same way that we would for any one of our members. And that's even just in a, in a, you know, the normal employee employment relationship, not even if we were providing a service like the Accolade service to them, which again, presents even further challenges in making sure that we keep that information completely private, secure, and accessed by only those who really, really need it, to perform their jobs.

[TRACEY]

In *Squid Game*, the contestants don't even know each other. They're identified by a number, not by a name. And of course, some of their backstories come out as the episodes go forward. But it's only because the contestants are initiating that contact with each other. Not because obviously the *Squid Game* company is encouraging it, they're really discouraging. It obviously in real life, companies are not putting numbers on their employees, and employees are, are able to share their personal lives with each other. What about salary information. Are employees permitted to discuss wage and benefit information with each other are companies allowed to sort of put a chilling effect on that?

[RICH]

That would be the kind of restriction that to me, doesn't really foster the kind of trusting relationship that we want. We're, we have a fair and equal pay policy, right? And, and we are looking at market data continually to make sure that and end the data of how our own employees are getting paid to make sure that we're doing as, as good as we possibly can compensate people appropriately for, for the roles that they have. And so, we're big believers in telling ourselves the truth and then trying to get to the best possible answers, you know, that matches both the employees needs and the companies.

[TRACEY]

Evan, do you want to chime in about that as well in terms of any NLRA implications?

[EVAN]

Yeah. I mean, that's, you know, certainly, you know, another piece to consider you see, you know, some of this on the internet, you know, people post, you know, communications from their employers, you know, threatening some pretty severe sanctions for, you know, discussing pay and things like that. It certainly raises, you know, some real problems under their National Labor Relations Act. You know, I mean, if you have sort of a blanket policy like that, then that's certainly going to attract their attention and, you know, it's not going to end well for you. You know, if the NLRB gets, gets wind to that, you know, their field offices. So yeah, there's certainly another piece to that that companies have to consider.

[TRACEY]

Sometimes companies are surprised to hear that because they think the National Labor Relations Act only applies if there's a union in the workforce. And that's not the case when it comes to the exercise of free speech among employees. One interesting twist on that concept of confidentiality is sort of this growing trend, prohibiting employers from asking applicants about their salary history when they're deciding about setting pay for those employees. What do you think about that in terms of employers not being able to even get that information before they make hiring decisions?

[RICH]

Yeah. Again, my opinion comes down to if your approach is to fairly compensate people and not have it be a pure zero-sum negotiation, then you're not so concerned about that, right? Because

you're, you're hiring somebody into a role. You have a sense of what the market bears for that role and you're trying to compensate that person as fairly as possibly within the market. That's your objective then. You're, you're not worried about that the person may have made less than market in their past job and therefore, you can take advantage of that in your negotiation with them, which I think is the concern of many of the legislators who are looking to pass those kinds of rules. Is that just because, and I think a lot of this has to do with, you know, underserved populations or, or systemic discrimination historically in the workplace where women, for example, would get paid less than men, right? And so, if you just propagate the person made less than their last job because that's the kind of company they work for. And now you, you add that to the information pool. It makes it potentially too easy for companies to take advantage of that. So, we, you know, we don't really concern ourselves that, and that's not our practice, even if it were to be permitted because we're trying to make sure that we fairly compensate people according to what the overall market standards are. And with those fair pay equity policies in mind.

[TRACEY]

So focus on the market rather than focus on what someone made in the past.

[RICH]

Yeah. And focus on equity, right. Focus on what is fair for the role that's being hired, irrespective of what that individual may have made previously and whether they're female, male, or, you know, person of color, all of that obviously has to be irrelevant in deciding or ought to be at least in the, in the pay sense, ought to be irrelevant in deciding what that rule's going to bear at our company.

[TRACEY]

And many companies still have lots of work to do in that area. I just heard recently that it's, I think it's been 40 days for women to have made the same amount of money that a male made in 2022 on day one. So, we're not there yet but hopefully, we'll get there. On the issue of discrimination, several states, such as California and New Jersey have enacted statutes, prohibiting parties from keeping settlements of discrimination and harassment claims confidential. And the, I think it's called the Enforced Arbitration Act was just recently passed prohibiting companies from requiring employees to arbitrate claims of sexual harassment. What do you think about this trend? Is it necessary to the employee's benefit that such information be kept from disclosure in the courts?

[RICH]

Yeah, I think there's, you know, any company who's facing one of these actions and, and has worked out a settlement with the employee values confidentiality, but I also understand the public policy behind these laws. And I would say for me, things happen in a company, right? You could even talk about cyber events or other things. I'm very much about what did you do to prepare and prevent that from happening? You know, what policies, procedures, training, and communication do we have to try to ever prevent harassment or discrimination from occurring in our business. Just as important is what you do when it does happen.

Any company would love to keep bad news confidential, but more important to me and what all companies should be saying to the world is we may have made a mistake. We believe that mistake is isolated. Here's what we're doing to prevent those mistakes, but here's also how we're responding to it to try to make sure it doesn't happen again. That's what's really critical, I think. And I think if more companies did that and focus less on pure confidentiality, we could really make advancements in areas like this that are just so key to, you know, I think getting the business world to a much better place and our society in general.

[TRACEY]

Maybe it's my pro-management bias though, but I would think that employees would have, would want to keep some of this information confidential. You know, some of these allegations can be very salacious, it's embarrassing, it's personal, and it may not be in the employee's best interest to sort of have their day in court. They may be better off in a private forum. I don't know whether passing laws, and not allowing that to happen is the way to go. Yeah. Evan, what are your thoughts on that?

[EVAN]

Yeah, I mean, it's a, yeah, it's a, I mean, it's a really double-edged sword. I mean, there is a, there is a fine line to walk there. You have sort of a the macro view of how having this stuff, public knowledge, or at least not forbidden from being confidential, you know, and how that sort of benefits society on a macro level versus the micro level sort of impact to the employee. I mean, in my opinion, I don't think there's a right or wrong answer. You know what I mean? I think the arguments on both sides are equally strong.

[TRACEY]

Probably depends on the case. Right? Depends on the fact of the case.

[EVAN]

Yeah, it's very case specific, you know, I just, I, I have, I can't say one approach is right or wrong because I can see it from both sides. I could see that a lot of employees, they would want to settle a case and still be able to talk about what happened to him. You know, if you take, you know, think about you an obvious example, you know, Harvey Weinstein, you know, I mean, I imagine there were a lot of people who would want to get a settlement from him, but then also be able to tell other people, “Hey, this is what happened to me, don't let it happen to you”. You know? And, and so I can certainly see that side, but I could also see, you know, people saying, no, I want this to be, I don't want people to know that this happened. You know, I'm, I'm embarrassed and, and this is my private life, and I don't want it exposed. It's so difficult to sort of legislate that. I'm not sure. And I don't know if those laws are specific to where it's, you know, it's like the employee's choice to whether there's a confidentiality provision or not. And maybe that's part of the answer is maybe that, you know, the victim gets to decide whether there's a confidentiality provision and the other side can't have that as a prerequisite to a settlement or a deal.

[TRACEY]

Okay. I know that the answer for the new federal law is that if the employee agrees, you know, but you can't require it as a binding arbitration agreement, but if an employee agrees in a specific case to arbitrate their claim, then it certainly can go forward in arbitration. It does seem to be a bit of a tension where an employee wants to keep it confidential, but it might be better for the societal good to get it out for the Harvey Weinstein type of case example. It's interesting.

[RICH]

I think there's a scope of confidentiality too. Meaning revealing that there was a discrimination claim of a certain type and then revealing the salacious details to me are two different things. And so maybe some of the sharpening of the pencil of these statutes would need to be around the nature of the information that would be discussed in any given case. But, no, it's a very difficult question on both sides. You can argue that any agreement that the employee enters as long as that agreement is not pre-entered before the event occurred, is based on that

[TRACEY]

Consent.

[RICH]

That person's, you know, that person's agreement. And so, It's a tough one to solve for sure.

[RICH]

Maybe for your next, sorry Evan. Maybe for the next podcast you can, you can cover the morning show, which obviously has a very Harvey Weinsteinesque spot line.

[TRACEY]

Funny that you say that, coming soon to a theater near you <laugh> or podcast near you.

[RICH]

There you go.

[TRACEY]

Switching gears for a second. I want to talk a little bit about COVID because COVID seems to impact every one of our podcast subject matters. A lot of companies moved to a remote workforce, obviously since COVID began in March 2020, and many of these companies continue to either have a remote workforce or work in a hybrid model. And, of course, some companies Accolade as a good example, had a remote component before COVID even hit. What are the particular concerns with confidentiality in a remote work environment and what can companies do to protect their confidential information, where you have employees working really across the country remotely?

[RICH]

You know, Accolade was one of those companies that had a hybrid workforce even before COVID obviously COVID forced us all out of the offices a hundred percent for a period of time. And we're starting to come back now, but you know, remote work presents a bunch of unique challenges, especially when the employees who are working remote are handling kind of confidential information and sense and information that we've been discussing. When you think about, well, what is that person's homework environment, right? Who else might be walking in and around the room where they're at. Who else might be able to sort of look over a shoulder and look at somebody's computer screen? What are a company's policies for printed documentation? We live in a very electronic world, but you know, there still are times and reasons for printing things and how do you enforce things like clean desk policies?

Probably the biggest fear that any company has that where confidential information is accessible through, you know, the computer system that they're providing to those employees working remotely is, is the mobile phone, high-resolution cameras on those mobile phones. There's no level of, you know, security controls on your system and monitoring that necessarily could prevent somebody from just taking a picture of their computer screen. Right. And so, you know, again, it comes back to the, to the culture of trust that you foster and having your employees be bought into that. So certainly, you have to do all of the controls, all of the homework space auditing, and COVID that made that even more complicated, because you can actually go to people's homes, had to do it sort of through the video camera, but you, you know, that's the table stakes. All of that has to be put in place. None of that will be successful if you don't foster that culture of trust in your business and have your employees be truly bought in on why these things are so important. And then, of course, arm them with the tools to go and, and live and model that in their own, in their own work life, which has really just become extremely important in a remote workforce world, which is now, you know, we were headed that direction before COVID. COVID has been a catalyst it's now really here to stay. For sure.

[EVAN]

Yeah, and another issue that I've seen come up is actually right in 2020. We had some employees at a client while they were at a competitor and then came to work for us. Long story short, they had some folks who complained that the VPN at the prior company was really slow and that accessing documents the through their our firm's is Imanage. but you know, through their document management system was really, really slow. And that sometimes, you know, they try to download a big spreadsheet and it would take, you know, 10 minutes or more to load. And, you know, I've had that same problem myself. You try to open a really big file through the VPN and it can really bog down and take a while to open. And so like, well I'll just save this locally, you know? And, and then I can access it much faster. And that's another thing that I've seen that's, you know, been a, been specifically tied to COVID. I just didn't really hear about that, but I'm sure I know people were doing that before, but it seems like it seemed that COVID certainly exacerbated that particular issue.

[TRACEY]

You know, I think that's a really good point and it's something I've seen also. And you know, it kind of gets down to the basics of, we need to give our employees the tools they need to do their jobs. And most employees really are acting in good faith to want to do their jobs, but it could be frustrating if they don't have those tools. And so. They'll look for workarounds too, make it work and those workarounds could be harmful to the company. So really need to give employees the right tools.

[RICH]

We've made this argument a long time ago, which is why I think we were very well prepared for the pandemic when it hit. You've got to think if you don't if you ignore or turn a blind eye to remote work or even just travel work right. When people are on the road and, and, and they suffer from the same issues and what you do is you fail to build the systems and the experience for your employees that, that enables them to do the right thing, just as your, you know, Evan and Tracy, you were describing. And so, for me, we, we very much think about, you know, remote work, as, you know when you buy the iPhone and you, you know, you open that case and, and there it is, it's wonderful and you turn it on and it just works, right? That experience of technology so that you don't have that VPN lag.

What that really enables us to do is have policies where we block people sharing files to external emails or things like Dropbox or other things like that. We block the ability to use the USB ports for the thumb drive. So, you can't offload that data. That's the table stakes I was talking about, but you only get to that point effectively, have your employees be happy with their work when you've given them the tools to not need those things because the VPN just works. And it doesn't, and it works seamlessly without lag and all that. When you start to introduce that into the system, you have one or the other thing. Employee workarounds, which lead to risks or dissatisfaction with their job, because they feel like they can't get their jobs done effectively. And those little things are often the frustration. We talk a lot about, even in office, if your seat doesn't work right, or the leg is broken, or it doesn't roll or whatever it is, that's bothering you that day then your work is going to suffer. And so, you, you have to pay attention to the little things as an employer, because it really matters in people's work life.

[TRACEY]

Well, this has certainly been an interesting topic. Confidentiality is something we could probably talk about all day. I do have one last question for both of you just to sort of bring it around to *Squid Game* again. In the context of that story and that company, what could the powers that be do differently to ensure confidentiality and the integrity of the game, so to speak without shooting their workers?

[RICH]

<laugh> That's a tough one because remember the game itself was eliminating individuals <laugh> by penalty of death.

[TRACEY]

Maybe they don't want to stop shooting, but maybe they want to shoot just the contestants, not the workers, right?

[RICH]

Yeah. We hope that most employers aren't, aren't using confidentiality as a way to do that kind of thing, Tracy, again, I think it comes back to a lot of the themes we've been talking about. Your, most employees want to do the right thing. Sure. You use zero trust sort of concepts because that's how you protect data most effectively. But at the end of the day, you really do want to trust your employees and you have to build that culture of trust. That's how you get employees engaged and understanding. One of the things I say a lot is privacy and security and confidentiality. I know we've been talking about this from a, you know, business confidential information perspective, but I think about them as very similarly related topics. It's not something we do off the side of our desks. It's something that is embedded in the culture of how we operate every second of the day.

And when you achieve that, and we are always striving to achieve that. Then some of these things get a little bit easier, but you always have to remain vigilant. But I think that that is how you take away the specter of, you know, operating at gunpoint, if you will, at propel of *Squid Game*, from the model. Your employees are fully invested and model that. Also, the side benefit of this, which is just so critical. You can talk about open door policies, but the way companies get in trouble, I think, is not that they've someone has screwed up that a mistake was made or that an employee even went rogue. That happens that's life. That's reality. You do everything you can to prevent it. If you don't actually model your open-door policy and have that information flow, when something goes wrong, even self-reporting our employees, I hope, feel really comfortable self-reporting that they made a mistake because we're not looking to fire people or in the *Squid Game* analogy, shoot them. What we're looking to do is understand that, so we can now fix the problem really rapidly and having that information move at light speed within the business is just so critical to being really good at your response to the bad thing that happened. Because bad things will happen, and you have to open your eyes to it. So, you really, I think that's how you fix at some level the *Squid Game* problem.

[TRACEY]

Well, Rich, this has certainly been an interesting conversation and Evan, and I just want to give you, you know, many, many thanks for joining us today. And thank you all for listening. We will speak to you next time on our *Hiring to Firing Podcast*. Thanks so much.

[RICH]

Thank you both for having me. Thank you.